A TRUST-AWARE DEEP REINFORCEMENT LEARNING FRAMEWORK FOR DETECTING INTERNAL ATTACKS IN IOBT NETWORKS

P. Rutravigneshwaran[1], V. Shanmugapriya[2]

Abstract

Internet of Battlefield Things (IoBT) is an emerging paradigm of the IoT that enhances military mission effectiveness through interconnected and autonomous battlefield devices. However, ensuring secure communication in IoBT networks remains a critical challenge due to the presence of resource constraints, dynamic topology, and internal routing attacks. The Routing Protocol for Low Power and Lossy Networks is commonly used for efficient routing in such environments, but it is highly susceptible to attacks such as black hole and selective forwarding, which degrade network reliability and performance. To address these limitations, this paper introduces a novel security framework that integrates Deep Reinforcement Learning (DRL) with trust management to enable efficient attack detection and secure routing in Internet of Battlefield Things (IoBT) networks. The proposed framework considers each network node as an intelligent agent that autonomously learns optimal routing strategies through continuous interaction with the dynamic network environment. A trust evaluation mechanism is incorporated into the reward function to penalize malicious behaviour and reinforce secure communication paths. The DRL-based model continuously adapts to changing network conditions and effectively identifies compromised nodes in real time. Experimental results highlight the superiority of the proposed approach over traditional machine learning methods. It delivers notable improvements in packet delivery ratio and detection accuracy, while simultaneously reducing routing overhead and end-to-end delay. These qualities position it as a robust, adaptive mechanism for safeguarding IoBT environments from internal threats.

Keywords : IoBT, IoT, RPL, Deep Reinforcement Learning (DRL), Trust Management, Intrusion Detection, Selective Forwarding Attack

Department of Information Technology[1]
Karpagam Academy of Higher Education (Deemed to be University)[1]
Coimbatore, Tamil Nadu, India[1]
rutra20190@gmail.com[1]

Department of Computer Science[2]
Sri Krishna Arts and Science College[2]
Coimbatore, Tamil Nadu, India[2]
shanmugapriyav@skasc.ac.in[2]

* Corresponding Author

I. INTRODUCTION

The Internet of Things (IoT) is an evolving paradigm in which conventional networked objects are extended to interact with physical entities such as home appliances, vehicles, industrial systems, and battlefield equipment. These interconnected "smart things" can sense their surroundings, communicate with nearby devices, and exchange information over the internet. Such entities may include physical objects, virtual components, and contextual events that collectively form an intelligent networked ecosystem. In military environments, the integration of IoT technologies significantly enhances operational capabilities, enabling improved situational awareness, faster decision-making, and higher mission efficiency. When IoT is deployed in defence applications, it forms a specialized framework known as the Internet of Battlefield Things (IoBT), where sensors, weapons, vehicles, wearable devices, robots, and unmanned systems collaborate to support mission-critical operations. The future battlefield is expected to consist of large-scale heterogeneous and highly dynamic intelligent systems. These devices perform diverse functions such as sensing, communication, actuation, coordination, and autonomous decision-making. Modern military systems are increasingly equipped with advanced sensor nodes capable of collecting, processing, and transmitting real-time battlefield data. However, alongside physical threats, IoBT networks are also vulnerable to cyber threats, where adversaries attempt to disrupt communication, manipulate data, or compromise system integrity. Unlike traditional IoT systems, IoBT operates in highly adversarial and unpredictable environments, making it significantly more vulnerable to security attacks. Malicious attackers can compromise IoBT networks through activities such as intercepting confidential communications, introducing fake or compromised nodes, manipulating mission-critical information, and performing attacks including black hole and selective forwarding attacks. Such security breaches severely affect the confidentiality, integrity, and availability of sensitive battlefield data. To mitigate these issues, this study presents an advanced security framework for IoBT environments that combines Deep Reinforcement Learning (DRL) with trust management techniques to enhance attack detection and secure routing. The proposed approach enables intelligent, adaptive, and autonomous detection of malicious behaviour while ensuring secure routing in highly dynamic battlefield the DRL-based

model dynamically identifies trustworthy nodes and isolates malicious entities to enhance overall network security and reliability.

The major contributions of this research are outlined below: An in-depth analysis of the Routing Protocol for Low-Power and Lossy Networks (RPL) within IoBT scenarios, including a detailed examination of potential adversarial threats and attack models. Development of a DRL-based security framework for adaptive attack detection and secure routing in IoBT networks. Design of a trust management model that integrates both direct trust and indirect trust metrics, considering Quality of Service (QoS) parameters and social trust characteristics. Introduction of a DRL-driven decision-making mechanism that dynamically evaluates node behaviour and predicts malicious activity based on learned trust patterns. Proposal of an intelligent filtering mechanism to eliminate dishonest or misleading trust recommendations from neighbouring nodes. Development of a secure routing strategy where DRL agents select optimal next-hop nodes based on trust evaluations and environmental feedback. Emphasis on the identification and prevention of critical IoBT threats, including black hole and selective forwarding attacks, to enhance overall network reliability and resilience. Demonstration that the proposed DRL-trust framework enhances authentication, attack isolation, and overall mission reliability in battlefield communication networks. Comparative performance analysis of the proposed framework with existing methods to demonstrate its superiority in security enhancement, adaptive decision-making, and efficient routing performance.

II. RELATED WORK

The development of the Internet of Things (IoT) has driven significant research focused on enhancing security and trust management, especially in critical domains like the IoBT. Because IoT networks are decentralized and often operate with limited resources, maintaining trustworthy node behaviour continues to be a major concern. This section surveys recent advancements in trust evaluation, including both cryptographic methods and reputation-based approaches.

In [1], the authors introduced an intrusion detection technique for 6LoWPAN networks aimed at preventing black hole attacks in RPL. Their method monitors node behaviour to detect suspicious activity, which is then verified by neighbouring nodes. Once confirmed, the root node removes the malicious entities. Although effective in identifying attackers, the approach does not provide a complete trust management framework.

In [2], researchers developed a reputation-driven trust model tailored for opportunistic IoT settings, where each node independently evaluates peer behaviour and classifies nodes as either trustworthy or malicious. This self-governing mechanism strengthens routing efficiency by steering data transmission away from untrustworthy participants. In [3], the authors developed a fuzzy logic to mitigate black hole and selective forwarding attacks. By evaluating node reliability and selecting safer routing paths, their system improves the success rate of packet delivery.

In [4], researchers designed a secure routing protocol that incorporates a lightweight remote attestation mechanism. By embedding attestation information into RPL control messages, the protocol verifies node integrity efficiently and strengthens network resilience.

Another study introduced a distributed trust evaluation approach for detecting black hole attacks. In this system, nodes independently compute trust values for their neighbours, which are later aggregated by a central entity such as a cluster head or border router. These aggregated scores help identify and isolate malicious nodes.

In [5], researchers proposed a trust-enhanced RPL protocol to defend against wormhole and grey hole attacks. Their method combines direct trust (based on node behaviour and rank consistency) with indirect trust obtained from neighbouring nodes, ensuring that routing decisions involve only reliable participants.

In [6], researchers proposed an energy-aware trust assessment framework designed specifically for military IoT environments. The model employs a hierarchical mechanism in which trust evaluation is initiated only upon the detection of abnormal activities, combining local node analysis with parent-node verification to minimize computational complexity and energy consumption.

In [7], researchers introduced a trust-aware routing mechanism for IoT and cyber-physical systems (CPS), where nodes are categorized as trusted, suspicious, or selfish based on past interactions. The model considers factors such as energy levels, network topology, channel conditions, and reputation to compute trust values, which are shared among neighbouring nodes to support secure routing decisions.

In [8], the authors proposed a hybrid security approach combining trust evaluation with cryptographic authentication to counter grey hole attacks. The model operates in multiple phases, including trust assessment, route validation, attack detection, and removal of malicious nodes, thereby improving overall system reliability.

In [9], researchers developed a cryptographic technique to address version number and rank attacks in RPL. This method uses hash chains to secure routing information, preventing manipulation while maintaining energy efficiency.

Despite the effectiveness of these methods, many approaches either rely heavily on cryptographic techniques or focus only on trust computation, which can introduce additional overhead. This proposed model classifies nodes as either trustworthy or malicious based on observed behaviour. Only verified nodes are allowed to participate in communication, while compromised nodes are excluded. This approach enhances both authentication and decision-making efficiency, making it suitable for dynamic and resource-constrained IoBT environments.

III. BACKGROUND

This section provides an overview of the Routing Protocol for Low-Power and Lossy Networks (RPL) and a brief introduction to the K-Nearest Neighbour (KNN) algorithm.

A. RPL Overview

RPL is a proactive routing protocol tailored for resource-constrained environments such as IoT and IoBT networks [11]. It is built upon a Destination-Oriented Directed Acyclic Graph (DODAG) structure, which organizes nodes hierarchically around a central root node. Data flows through the network via parent-child relationships, with sensor nodes forwarding packets to the root through their preferred parent. The root node manages outbound routing toward destination networks and supports communication in both upward and downward directions. Multiple RPL instances, each containing one or more DODAGs, can coexist within the same network. To prevent routing loops, RPL assigns each node a rank value reflecting its relative distance from the root. Since every node's rank must exceed that of its parent, loop-free routing is inherently enforced. The protocol further supports network resilience through local and global repair mechanisms that respond to link failures and topology changes. RPL operates in two modes: storing and non-storing. Storing mode enables nodes to maintain local routing tables for efficient forwarding, while non-storing mode offloads all routing decisions to the root node. Root nodes typically operate in storing mode with full topological awareness, and border routers may additionally manage routing for specific segments of the network.

B. Overview of Deep Reinforcement Learning (DRL) Algorithm

DRL is an advanced machine learning paradigm that combines deep neural networks with reinforcement learning principles to support autonomous decision-making in complex, dynamic settings. Its theoretical foundation is rooted in the Markov Decision Process (MDP), formally represented as:

$$MDP = S, A, P, R, \gamma \quad (1)$$

where S denotes the set of states, A represents the set of actions, $P(s' \mid s, a)$ defines the state transition probability, $R(s, a)$ is the reward $\gamma \in [0,1]$ function, and is the discount factor that determines the importance of future rewards. Top of Form

In this proposed work, MDP is utilized as the underlying framework due to its ability to efficiently model sequential decision-making in dynamic environments. It is computationally tractable, easy to formulate, and well-suited to capturing optimal policy learning while maintaining satisfactory prediction performance.

IV. DRL TRUST MODEL (DEEP REINFORCEMENT LEARNING TRUST MODEL)

The primary objective of this paper is to develop a comprehensive trust-based model to mitigate black hole attacks and selective forwarding attacks in battlefield environments. The proposed model assesses the trustworthiness of each node by analysing its historical interactions and behavioural patterns to effectively identify malicious nodes within the network. Although malicious nodes may exhibit various forms of harmful behaviour, this study primarily focuses on two widely observed attacks in IoBT environments: black hole attacks and selective forwarding attacks [12]. While lightweight authentication protocols and encryption techniques can help prevent external threats, they are often insufficient to defend against internal attacks. Such attacks are typically launched by legitimate nodes that possess valid identities within the network, making detection more challenging. In this context, a trust-aware mechanism becomes highly effective for enhancing network security. The proposed model incorporates relevant trust metrics that reflect the impact of these attacks on network performance and reliability. The elimination of malicious IoBT nodes ensures improved security and reliability in battlefield communications. Furthermore, the model guarantees data authenticity by allowing only trusted and authenticated nodes to participate in the routing process within the IoBT environment [13].

A. Network Model Assumptions

The proposed DRL Trust framework is developed under a set of assumptions specific to the IOBT environment, as outlined below:

The considered network operates in a pure IoBT battlefield scenario, where various IoBT devices are deployed on soldiers, military vehicles, and other military assets. These devices are required to communicate and cooperate effectively to ensure successful mission execution. The network topology is highly dynamic, as soldiers and vehicles frequently move across different operational regions, leading

to continuous changes in network structure and connectivity.

The IoBT network is considered heterogeneous, as the participating nodes possess varying levels of energy resources, memory size, computational capability, storage capacity, and communication protocols. Every network region is assumed to contain a resource-rich device that operates as a border root node, usually controlled by a commander to support efficient communication and network coordination. The system follows a decentralized architecture, where no single centralized trusted authority exists. Therefore, each IoBT node must independently evaluate its surrounding environment and maintain records of both trusted and potentially malicious nodes for future interactions. IoBT devices are characterized by constrained resources such as limited energy supply, memory capacity, and processing capability. These resources are continuously consumed by sensing operations, data analysis, monitoring functions, and communication activities, making the devices more vulnerable to compromise by adversarial entities. Compromised or malicious nodes within the network can engage in harmful actions, including packet dropping and selective forwarding attacks, which disrupt normal communication processes and threaten the reliability of mission-critical battlefield operations.

B. Adversary Model

In this work, an IoBT node is considered malicious when it intentionally drops data packets either completely or selectively during transmission. In battlefield environments, such malicious behaviour can lead to critical disruptions in network communication and mission execution [14].

For instance, soldiers may transmit mission-critical information to the commander through intermediate IoBT nodes. However, if any of these intermediate nodes behave maliciously, they may drop or selectively forward the transmitted data, resulting in communication failure, mission disruption, or even endangering soldiers' lives. Nodes that have been infiltrated and manipulated by adversarial entities are classified as malicious nodes. These compromised nodes are primarily deployed with the intent to undermine the efficiency of the routing protocol and interfere with the operational continuity of mission-critical functions within the IoBT network.

C. Black Hole Attack

A black hole attack occurs when compromised nodes deliberately discard all received data packets rather than relaying them to adjacent nodes in the network. This malicious behaviour results in total packet loss, causing severe disruption to network communications and significantly deteriorating the routing performance of the IoBT infrastructure.

D. Selective Forwarding Attack

A selective forwarding attack differs from a black hole attack in that the malicious node does not suppress all traffic uniformly. Rather, it selectively transmits certain packets while covertly discarding others. This strategy is aimed at destabilizing routing reliability, weakening data transmission pathways, and potentially disconnecting targeted nodes or communication protocols from the broader network [15].

Figure 1. A Standard RPL Network Operating in the Absence of Attacks.

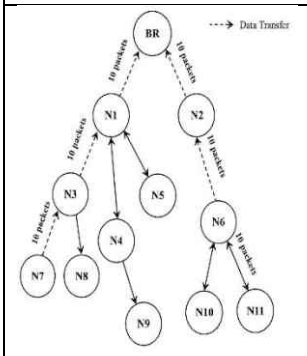

Figure 2. A Standard RPL Network Operating in the Presence of Blackhole and Selective Forwarding Attacks.

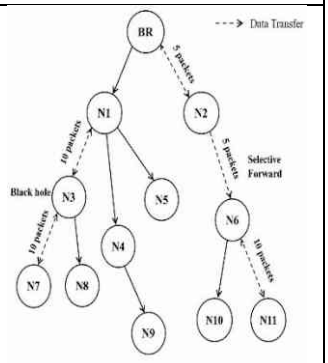

Figure 1 depicts an RPL network operating normally in the absence of any malicious activity. Nodes N7 and N11 send data packets toward the Border Root through intermediate nodes. As every node in the network is trusted and authenticated, all packets are forwarded seamlessly and arrive at the Border Root without any loss.

Figure 2 illustrates the RPL network under the presence of black hole and selective forwarding attacks. Here, nodes N7 and N11 route their data through nodes N3 and N6. Node N3 conducts a black hole attack by dropping all incoming packets instead of forwarding them to its neighbouring node N1. In contrast, node N6 performs a selective forwarding attack by intentionally dropping only certain packets while allowing others to pass through, making the attack less noticeable.

Both attacks are highly critical in battlefield network environments, where secure and reliable communication is essential. Mission-critical data is often transmitted between soldiers and commanders through multiple intermediate nodes. If any of these nodes behave maliciously-either by completely discarding packets or selectively filtering them—the information may not reach its intended destination. Such disruptions can jeopardize soldiers' safety and significantly increase the likelihood of mission failure.

The main goal of the DRL Trust framework is to efficiently identify black hole and selective forwarding attacks, detect the malicious nodes involved in these

activities, and eliminate or isolate them from the network to maintain secure, stable, and reliable communication.

V. TRUST MANAGEMENT

A key function of trust management is to gather the relevant information required for accurate trust evaluation [26]. Trust is generally defined based on multiple factors such as Quality of Service (QoS), honesty, availability, risk, and related attributes. It represents the level of confidence one node has in another, derived from observations of its past behaviour [16].

The proposed trust model is specifically developed for IoBT (Internet of Battlefield Things) applications. These direct trust values are then shared with other nodes as recommendation values, which are used to calculate indirect trust. Recommendation trust managers aggregate these values, eliminate unreliable or dishonest recommendations, and compute indirect trust using only the trustworthy inputs. By combining both direct and indirect trust metrics, DRL-based algorithms are employed to predict node behaviour effectively.

A. DRL-Trust Model

The DRL-Trust model evaluates node trustworthiness by integrating both direct and indirect trust components. For direct trust, metrics such as forwarding reliability, contact intimacy, and honesty are combined using a weighted average approach. Indirect trust is derived by collecting recommendation values from neighbouring nodes that share common interactions with the target node.

To predict node activities, the model employs the K-Nearest Neighbours (KNN) algorithm, utilizing historical direct and indirect trust values. In battlefield scenarios, relying solely on Quality of Service (QoS) metrics is insufficient for assessing trust, as communication reliability directly impacts mission success and human safety [17].

QoS trust represents a node's capability to reliably forward data packets to their intended destinations and is obtained from communication and network performance indicators. In this model, forwarding reliability is used as the primary QoS metric. Social trust, on the other hand, reflects the relationship between the entities controlling IoT nodes and is evaluated using factors such as intimacy, honesty, and centrality. The proposed model specifically uses contact intimacy and honesty to quantify social trust.

B. Direct Trust

Direct trust is evaluated using observations obtained from firsthand interactions between nodes. It reflects the level of trust one node places in another based on their direct relationship and past behaviour. The calculation incorporates multiple trust attributes, derived from repeated interactions within the network environment [18]. As it is based on information gathered from neighbouring nodes, direct trust is considered reliable and readily accessible, since it relies on firsthand evidence rather than external inputs. In the DRL-Trust model, direct trust is computed using key metrics such as forwarding reliability, contact intimacy, and honesty. These metrics are specifically chosen due to their significant influence in identifying and mitigating black hole and selective forwarding attacks [19].

IoBT node i evaluates the direct trust value of IoBT node j as follows

$$DTi,j(t) = w1.FRi.j(t) + w2.CIi,j(t) + w3.Hi,j(t) \quad (2)$$

FRi.j(t) - Forwarding Reliability at 't' time.

CIi,j(t) -Contact Intimacy at 't' time

H(t)- Honesty at 't' time (based on number of positive and negative interaction between node i and node j)

DTi,j(t) — The direct trust that node i holds toward node j is computed by leveraging historical interaction data and firsthand behavioural observations. Each of the trust metrics adopted within this proposed model is described in detail as follows.

C. Forwarding Reliability

This metric evaluates Quality of Service (QoS) trust by measuring a node's ability to forward data packets accurately without loss or alteration. A higher rate of packet drops or data tampering indicates reduced reliability [20]. Selfish nodes may intentionally discard packets to conserve energy, while malicious nodes may drop or modify packets to disrupt operations and degrade overall network performance. Therefore, forwarding reliability serves as a key indicator for distinguishing trustworthy nodes from selfish or malicious ones.

It is defined as follows

$$FR_{(}i,j_{)}(t) = CFP_{(}i,j_{)}(t) / RP_{(}i,j_{)}(t) \quad (3)$$

CFPi,j(t) — Refers to the overall number of data packets that node j has effectively forwarded at time t.

RPi,j(t) — Indicates the total count of data packets received at node j during time period t.

FRi.j(t)-Forwarding Reliability of node j measured by node I.

After every communication, node i measure the forwarding reliability of its neighbour node j through acknowledgment [31].

D. Contact Intimacy

This metric is an important factor in evaluating social trust. It quantifies the closeness between two nodes based on the frequency of their interactions [21]. A higher number of contacts between a pair of nodes indicates stronger intimacy. Nodes with greater contact intimacy are more likely to reliably forward data packets, as their interaction history reflects a stronger level of association. Contact intimacy is

calculated as follows :

$$CI(i,j)(t) = CF(i)(t) / TCF(i)(t) \quad (4)$$

CFi,j(t) - represents the contact frequency between node iii and node j at time t.

TCFi(t) - □ Total number of contacts established by node iii with all neighbouring nodes.

E. Honesty

Honesty is a key social trust metric used to evaluate the trustworthiness of a node. It helps identify potential attackers by examining deviations or abnormal patterns in node behavior [22]. This metric is quantified based on the number of successful (positive) and unsuccessful or suspicious (negative) interactions between nodes. The honesty is defined as follows:

$$H(i,j)(t) = \frac{\alpha(i,j)(t)}{(\alpha(i,j)(t) + \beta(i,j)(t))} \quad (5)$$

αi,j(t)-Represents the cumulative number of successful and positively acknowledged communication interactions recorded between nodes i and j up to time t.

Bi,j(t) - Total count of failure communications.

αi,j(t)+βi,j(t) represents the total number of positive and negative communication interactions.

I – Node being evaluated, j – Node performing the evaluation

F. Indirect Trust

Indirect trust, often referred to as second hand information, becomes particularly useful when nodes have little or no direct interaction, or when available interactions are insufficient to reliably assess trustworthiness [26]. This form of trust is obtained from recommendations provided by other trusted third-party nodes. Recommendation-based trust is therefore a crucial component of any trust evaluation framework [23].

In the DRLTrust model, a node seeking to evaluate another node requests recommendation values from its neighbouring nodes. As a result, it receives numerous responses, which may include inputs from both honest and malicious nodes. In a distributed network environment, to address this issue, the proposed model incorporates a filtering mechanism to distinguish and eliminate dishonest recommendations before computing indirect trust [24].

Algorithm 1: Indirect Trust Computation

Step 1: The evaluated node requests recommendation trust values from its neighbouring nodes regarding the target node.

Step 2: The evaluated node collects recommendation responses from its neighbours.

Step 3: Form the recommendation trust set: $RT_i = \{RT_1, RT_2, RT_3, \ldots, RT_n\}$.

Step 4: Compute the median value m of the recommendation trust set.

Step 5: Calculate the deviation of each recommendation value from the median using a one-dimensional Euclidean distance.

Step 6–9: For each recommendation (i = 1 to n), compute $d_i = |RT_i - m|$ and accumulate the total distance.

Step 10: Determine the mean of the distance values: mean = $(\Sigma d_i)/n$.

Step 11–16: For each recommendation, if $d_i \leq$ mean, consider it as a valid (honest) recommendation; add it to the total recommendation trust (TRT) and increment the count of valid nodes (j).

Step 17: Compute indirect trust as IT = TRT / j.

Step 18: End.

This algorithm identifies and removes unreliable recommendations by leveraging statistical measures such as median, mean, and Euclidean distance. First, the median of the recommendation set is determined, and the distance of each recommendation from this median is calculated. The average of these distances is then used as a threshold [25]. Any recommendation with a deviation greater than the mean is treated as dishonest and excluded. The final indirect trust value is computed by averaging only the filtered, trustworthy recommendations.

VI. ISOLATION OF MALICIOUS NODES IMPLEMENTATION OF THE DRL ALGORITHM

During the classification phase, the evaluating node utilizes the current direct and indirect trust values to determine whether another node exhibits trustworthy or malicious behaviour.

Algorithm 2: Node Behaviour Classification (Trusted or Malicious)

Step 1: Calculate the similarity between the current trust data and all stored training samples using a distance measure (e.g., Euclidean distance).

Step 2: Select the value of K (number of nearest neighbours).

Step 3: Rank all distances in ascending order and identify the K closest neighbours.

Step 4: Discard all data points beyond the selected K nearest neighbours.

Step 5: Classify the node's behaviour by considering the majority category (trusted or malicious) among its nearest neighbouring nodes.

Once a node is identified as malicious, it is immediately excluded from the battlefield network and barred from taking part in any future mission-related activities. The IoBT root node, typically managed by the commander, broadcasts information about detected malicious nodes to the rest of the network [26]. This enables other nodes to sever communication links with those nodes, effectively isolating them. As a result, only trusted nodes remain active, ensuring secure and authenticated communication within the battlefield network. The comprehensive architectural

framework of the DRL-Trust model is presented and depicted in Figure 3.

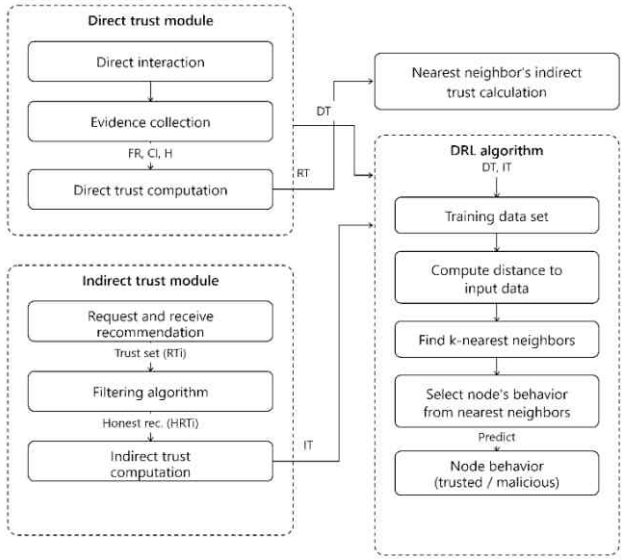

Figure 3. The overall design of the DRLTrust Model

VII. SIMULATION RESULTS AND DISCUSSION

A. Performance Evaluation Metrics

The DRLTrust model is implemented and tested using the Contiki 3.0 operating system along with the Cooja network simulator. TMote Sky sensor nodes are used as the mote type for the simulation. The simulation parameters adopted for evaluating the DRLTrust model are presented in the following table. The simulation parameters that have been defined and configured for the proposed DRLTrust model are documented and presented in Table 4.

Table 1. Simulation Parameters for the Proposed DRLTrust Model

System Parameters	Values
Number of nodes	50
Mote Type	TMote Sky
Simulation Time	3600Sec
Network Coverage Area	300mx300m
Data Rate	3072bps
Data Packet Size	64 byte
Traffic	UDP
Mac Layer	IEEE 802.15.4
Communication Range	50m
RPL Parameter	MinHop-RankIncrease=256
Routing Protocol	DRLTrust, RPL, David et al., 2017

B. Simulation Results

The DRLTrust model is evaluated across the following experimental scenarios to determine its overall effectiveness:

As the model targets malicious nodes executing black hole and selective forwarding attacks, analysing the influence of these threats is a critical step. This is accomplished by progressively increasing the share of malicious nodes and observing the resulting packet drop ratio in the RPL network. The DRLTrust model is benchmarked against both the conventional RPL protocol and the approach developed by David et al. (2017), with evaluation based on packet forwarding ratio, average delay, and routing overhead metrics. The proportion of malicious nodes is incrementally raised to evaluate and contrast the detection accuracy achieved by the DRLTrust model with that of the method presented by David et al. (2017).

This scenario examines the behaviour of the network under the standard RPL protocol with a varying number of malicious nodes. The results shown in Figure 5 indicate that as the proportion of malicious nodes increases, the packet drop rate also rises significantly.

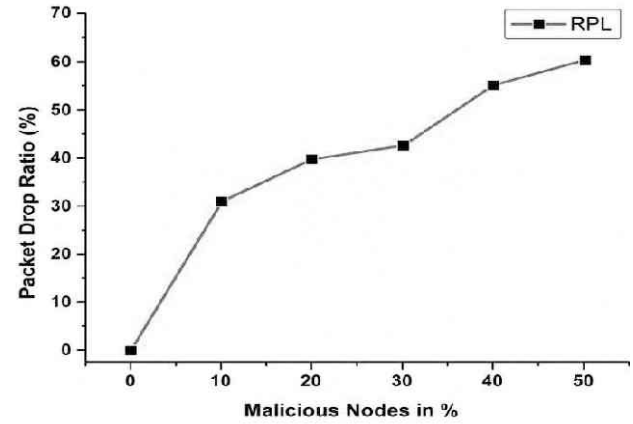

Figure 4. presents the effect of malicious nodes within a network using the standard RPL routing approach.

Scenario 2: This simulation evaluates the proposed DRLTrust model by comparing its forwarding ratio, average delay, and routing overhead with those of RPL and the approach by David et al. (2017).

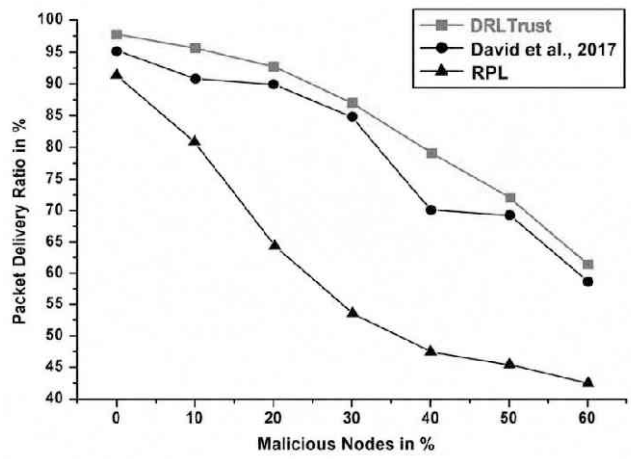

Figure 5. Packet Delivery Ratio

B. Packet Delivery Ratio:

The Packet Delivery Ratio (PDR) measures the proportion of packets successfully delivered to the destination node relative to the total number of packets originally transmitted by the source node [27]. It serves as a critical benchmark for assessing the effectiveness of the DRLTrust model, capturing packet delivery efficiency at both node-specific and network-wide levels. Protocol performance is evaluated by gradually increasing the fraction of malicious nodes from 0% to 60%.

Figure 6 illustrates the packet delivery performance of DRLTrust, RPL, and the model proposed by David et al. (2017). The results indicate that the DRLTrust model achieves a higher delivery ratio compared to the other approaches. This improvement is mainly because the proposed model utilizes the correct forwarding ratio rather than relying solely on packet delivery ratio for trust evaluation [28]. While the method by David et al. depends on a single trust parameter (packet delivery ratio), the proposed approach incorporates multiple trust factors such as forwarding ratio (FR), consistency index (CI), and honesty (H). By using these multiple metrics, the system can effectively detect and eliminate malicious nodes involved in black hole and selective forwarding attacks. Consequently, only reliable nodes participate in routing, which enhances overall packet delivery performance.

D. Average Delay:

Average delay refers to the mean temporal duration required for a data packet to complete its journey from the originating source node to the intended destination node. It constitutes a fundamental performance indicator in the assessment and comparison of routing protocol efficiency. The introduction of malicious nodes within the IoBT network environment typically contributes to a measurable escalation in overall transmission delay, adversely affecting communication performance [29].

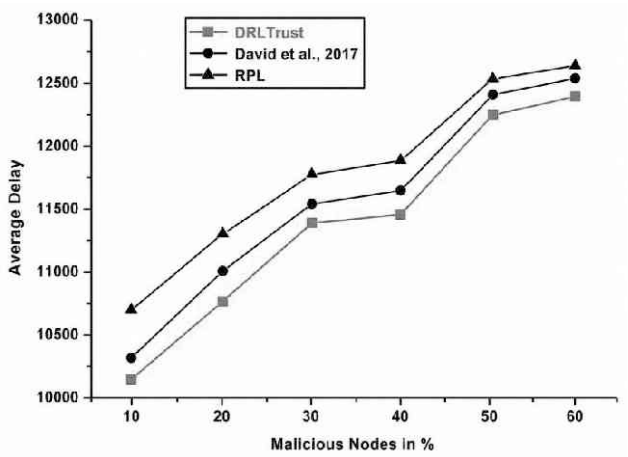

Figure 6. Average Delay

Figure 6 compares the delay performance of DRLTrust, RPL, and the approach proposed by David et al. (2017) as the percentage of malicious nodes increases. The findings indicate that the DRLTrust model achieves lower delay than the other two methods. This is mainly because it can identify malicious nodes at an earlier stage compared to the model by David et al. The proposed approach utilizes the DRL-based machine learning algorithm to classify node behaviour efficiently and accurately. It is capable of detecting malicious nodes with a minimal amount of training data and removing them from the network [30]. Consequently, only trusted IoBT nodes are selected for routing, which helps in minimizing delay. In contrast, RPL does not include any mechanism for detecting malicious nodes, resulting in higher delay due to the involvement of compromised nodes in the communication process.

E. Routing Overhead:

Routing overhead is defined as the ratio of control (routing) packets to actual data packets transmitted. Figure 8 illustrates the routing overhead of the DRLTrust model compared with RPL and the model proposed by David et al. (2017) under different proportions of malicious nodes. It is evident that DRLTrust consistently produces lower routing overhead than the other two approaches. Attacks such as black hole and selective forwarding disrupt normal network operations by causing malicious or selfish nodes to intentionally drop packets. This leads to an increase in control traffic, thereby raising routing overhead and reducing network stability. The DRLTrust approach mitigates this issue by accurately detecting and isolating nodes involved in such attacks, resulting in a more stable network and reduced routing overhead.

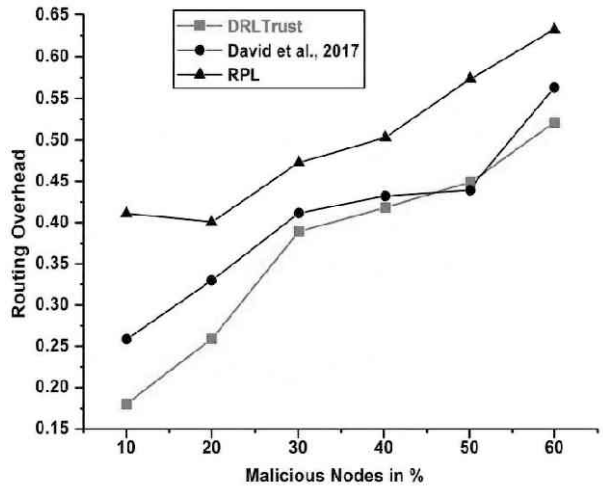

Figure 7. Routing Overhead

Figure 8 presents a comparison of detection accuracy between the DRLTrust model and the model proposed by

David et al. However, DRLTrust maintains significantly higher accuracy than the model by David et al. This improvement is attributed to the incorporation of a filtering mechanism that eliminates dishonest recommendations. Indirect trust is derived exclusively from reliable recommendations, while direct trust is computed using multiple metrics, including forwarding reliability, contact intimacy, and node honesty, ensuring more dependable trust evaluation. In addition, the Deep Reinforcement Learning (DRL) component enhances the model's ability to predict node behaviour, further improving detection performance. In contrast, the model by David et al. relies solely on forwarding behaviour for trust assessment, which limits its accuracy.

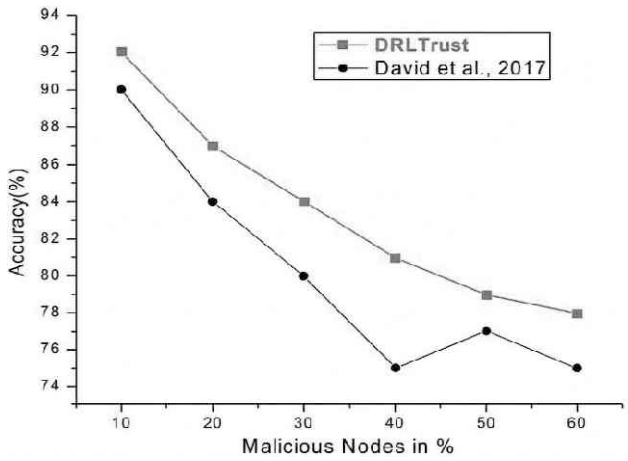

Figure 8. Accuracy

VIII. CONCLUSION

Future Internet of Battlefield Things (IoBT) systems will be increasingly shaped by advancements in cyber warfare and artificial intelligence, where security becomes a critical factor for successful deployment. Among various security requirements, authentication plays a vital role in ensuring that only legitimate nodes participate in communication, which is especially important in IoBT environments due to their direct impact on soldiers' safety. However, IoBT devices are typically resource-constrained, making them more vulnerable to attacks. Common threats such as black hole and selective forwarding attacks can severely disrupt network performance. Conventional security mechanisms are often unsuitable for IoBT networks, as they demand significant computational resources and rely on centralized infrastructure for key management. In contrast, trust-based approaches are more appropriate for distributed and dynamic environments like IoBT. To address these challenges, the model establishes trust by incorporating both direct interactions and recommendations from neighbouring nodes. Direct trust is calculated using a weighted-average approach based on parameters such as forwarding reliability, contact intimacy, and node honesty. To improve reliability, a novel filtering mechanism is introduced to remove dishonest or biased recommendations, ensuring that only credible inputs contribute to indirect trust computation.

Furthermore, the proposed framework integrates a Deep Reinforcement Learning (DRL) algorithm to accurately predict node behaviour based on the computed direct and indirect trust values. Each node continuously maintains historical interaction information, including trust evaluations and observed behavioural characteristics, which are subsequently utilized as training data for the DRL model.

Based on this information, the system can effectively classify and predict the trustworthiness of nodes. One of the key advantages of the DRL approach is its ability to achieve accurate predictions with relatively small training datasets, while remaining computationally efficient and fast.

The DRLTrust model is integrated into the RPL protocol, and its performance is evaluated using the Cooja simulator. Experimental results demonstrate that the proposed model outperforms traditional trust-based RPL approaches, particularly under varying levels of malicious node presence, confirming its effectiveness in enhancing network reliability and security.

REFERENCES

[1] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of “Internet of Things”. First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435.

[2] Glowacka, J., Krygier, J., &Amanowicz, M. (2015). A trust-based situation awareness system for military applications of the internet of things. 2015 IEEE 2nd World Forum on the Internet of Things (WF-IoT). doi:10.1109/wf-iot.2015.7389103.

[3] Suri et al., “Analyzing the applicability of Internet of Things to the battlefield environment,” in Proc. Int. Conf. Military Commun. Inf. Syst. (ICMCIS), Brussels, Belgium, May 2016, pp. 1–8.

[4] A. Kott, A. Swami and B. J. West, "The Internet of Battle Things," in Computer, vol. 49, no. 12, pp. 70-75, Dec. 2016, doi: 10.1109/MC.2016.355.

[5] Abuzainab, N., & Saad, W. (2018). Dynamic Connectivity Game for Adversarial Internet of Battlefield Things Systems. IEEE Internet of Things Journal, 5(1), 378–390. doi:10.1109/jiot.2017.2786546.

[6] Patel, H. B., &Jinwala, D. C. (2019). Blackhole Detection in 6LoWPAN Based Internet of Things: An Anomaly Based Approach. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON).

doi:10.1109/tencon.2019.8929491.

[7] Kandhoul, N., Dhurandher, S. K., &Woungang, I. (2019). T_CAFE: A Trust based Security approach for Opportunistic IoT. IET Communications. doi:10.1049/iet-com.2019.0657.

[8] Airehrour D, Gutierrez JA, Ray SK (2017) A trust-aware RPL routing protocol to detect black hole and selective forwarding attacks. J Telecommun Digital Econ 5(1):50–69. https://doi.org/10.18080/ jtde.v5n1.88.

[9] Conti M, Kaliyar P, Rabbani MM, Ranise S (2018) SPLIT: a secure and scalable RPL routing protocol for Internet of Things. In: 2018 14th International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob). IEEE, pp 1–8.

[10] A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on. IEEE, 2017, pp. 1169–1176.

[11] Mehta, R., & Parmar, M. M. (2018). Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks. 2018 3rd International Conference for Convergence in Technology (I2CT). doi:10.1109/i2ct.2018.8529426

[12] Lim, J., Ko, Y.-B., Kim, D., & Kim, D. (2018). A Stepwise Approach for Energy Efficient Trust Evaluation in Military IoT Networks. 2018 International Conference on Information and Communication Technology Convergence (ICTC). doi:10.1109/ictc.2018.8539353.

[13] T.Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks",https://tools.ietf.org/html/rfc6550, 2012.

[14] Le, A., Loo, J., Luo, Y., &Lasebae, A. (2011). Specification-based IDS for securing RPL from topology attacks. 2011 IFIP Wireless Days (WD). doi:10.1109/wd.2011.6098218.

[15] Mathur, A., Newe, T., & Rao, M. (2016). Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT. Sensors, 16(1), 118. doi:10.3390/s16010118

[16] Hatzivasilis G, Papaefstathiou I, Manifavas C (2017) SCOTRES: secure routing for IoT and CPS. IEEE Intern Things J 4(6):2129–2141

[17] Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., &Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing. doi:10.1007/s11227-019-03137-5

[18] A. Dvir, T. Holczer, and L. Buttyan. Vera - version number and rank authentication in RPL. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems.

[19] Ao Li, Lirong Wang, Yunzhou Shi, Minghui Wang, Zhaohui Jiang, &Huanqing Feng. (2005). Phosphorylation Site Prediction with A Modified k-Nearest Neighbor Algorithm and BLOSUM62 Matrix. 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference. doi:10.1109/iembs.2005.1615878.

[20] Hu, L.-Y., Huang, M.-W., Ke, S.-W., & Tsai, C.-F. (2016). The distance function effect on k-nearest neighbor classification for medical datasets. Springer Plus, 5(1). doi:10.1186/s40064-016-2941-7.

[21] Guo, G., Wang, H., Bell, D., Bi, Y., & Greer, K. (2003). KNN Model-Based Approach in Classification. Lecture Notes in Computer Science, 986–996. doi:10.1007/978-3-540-39964-3_62.

[22] Saini, I., Singh, D., & Khosla, A. (2013). QRS detection using K-Nearest Neighbor algorithm (KNN) and evaluation on standard ECG databases. Journal of Advanced Research, 4(4), 331–344. doi:10.1016/j.jare.2012.05.007.

[23] Denko, M. K., Sun, T., & Woungang, I. (2011). Trust management in ubiquitous computing: A Bayesian approach. Computer Communications, 34(3), 398–406.

[24] Kamble, A., Malemath, V. S., & Patil, D. (2017). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI). doi:10.1109/etiict.2017.7977006.

[25] A.Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing (ICPC). DOI:10.1109/pervasive .2015.7087034.

[26] Babu, S. S., Raha, A., &Naskar, M. K. (2011). Geometric mean-based trust management system for WSNs (GMTMS). 2011 World Congress on Information and Communication Technologies. doi:10.1109/wict.2011.6141286.

[27] Jiang, J., Han, G., Wang, F., Shu, L., &Guizani, M. (2015). An Efficient Distributed Trust Model for Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 26(5), 1228–1237. doi:10.1109/tpds.2014.2320505

[28] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, vol. 13, no. 4,

2011, pp. 562-583.

[29] Guo, J., Chen, I.-R., & Tsai, J. J. P. (2017). A survey of trust computation models for service management in internet of things systems. Computer Communications, 97, 1–14. doi:10.1016/j.comcom.2016.10.012.

[30] Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H.-M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7), 2096–2114. doi:10.1016/j.adhoc.2012.02.009.